FORM PTO-1390 (REV. 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER **2345/86**

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/381056

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED:
PCT/EP98/07984	09 December 1998 (09.12.98)	12 January 1998 (12.01.98)

TITLE OF INVENTION
A METHOD FOR GENERATING ASYMMETRICAL CRYPTOKEYS AT THE USER'S LOCATION

APPLICANT(S) FOR DO/EO/US
MERTES, Paul; METTKEN, Werner

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until he expiration of the applicable time limit set in 35 U.S.C 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). unsigned
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: PCT Request RO/101 and Return Receipt Postcard.

Express Mail No.: EL179668701US

420 Rec'd PCT/PTO 13 SEP 1999

U.S. APPLICATION NO. if known, see 37 C.F.R. 1.5	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/381056	PCT/EP98/07984	2345/86

17. ☒ The following fees are submitted:	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)):		
Search Report has been prepared by the EPO or JPO $840.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) . . . $670.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $760.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $970.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

Claims	Number Filed	Number Extra	Rate		
Total Claims	3 - 20 =	0	X $18.00	$0	
Independent Claims	1 - 3 =	0	X $78.00	$0	
☐ Multiple dependent claim(s) (if applicable)			+ $260.00	$	
			TOTAL OF ABOVE CALCULATIONS =	$840	
☐ Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$	
			SUBTOTAL =	$840	
☐ Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$	
			TOTAL NATIONAL FEE =	$840	
☐ Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property +				$	
			TOTAL FEES ENCLOSED =	$840	
			Amount to be: refunded	$	
			charged	$	

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $840.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

Richard L. Mayer
SIGNATURE

By: Richard L. Mayer (Reg. No. 41,172)

SEND ALL CORRESPONDENCE TO:

Kenyon & Kenyon
One Broadway
New York, New York 10004

Richard L. Mayer, Reg. No. 22,490
NAME

9/13/99
DATE

[2345/86]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Paul MERTES et al.
Serial No.	:	To Be Assigned
Filed	:	Herewith
For	:	A METHOD FOR GENERATING ASYMMETRICAL CRYPTOKEYS AT THE USER'S LOCATION
Group Art Unit	:	To Be Assigned

Assistant Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

SIR:

Please amend the above-identified application before examination as follows:

In The Specification:

On page 1, line 1, change "Background Information" to --Background Information--.

On page 1, line 3, before "invention" insert --present--.

On page 1, line 3, change "of the type described in more detail in" to --.--.

On page 1, delete line 4 and in its place insert --Asymmetrical cryptological methods are described generally in--.

On page 1, line 5, after "1997." insert --The present invention relates in particular to all forms of asymmetrical cryptological methods. Such methods are used, for example, in ATM cards/bank transactions, access controls to networks/databases, entry controls to buildings/rooms, digital signatures, digital IDs/patient cards, etc.--.

On page 1, line 20, after "Internet." insert --In generating asymmetrical cryptokeys in the handwriting of the user, signature and encryption keys are necessary, and in personalizing and certifying, reliable connections to a Trust Center are necessary. If users wish to generate their own keys, particularly cryptokeys, security problems arise.--.

On page 1, line 21, insert --Summary Of The Invention--.

On page 1, delete line 26.

On page 2, delete line 1.

On page 2, delete line 3 and in its place insert --Detailed Description--.

On page 4, line 1, change "Patent Claims" to --What Is Claimed Is:--.

In The Claims:

Please cancel claims 1-3 and add new claims 4-6 as follows:

--4. (New) A method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center, the method comprising the steps of:

causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

producing the at least one encryption key pair including a public part and a secret part;

marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

unequivocally assigning the at least one encryption key pair to the user;

causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair;

encrypting the new certificate using the public part of the at least one encryption key pair; and

causing the trust center to transmit the encrypted new certificate to the user.

5. (New) The method according to claim 4, wherein:

the step of causing the trust center to provide the user with components for producing at least one encryption key pair includes the step of providing the user with components for producing at least one additional signature key pair,

the step of producing the at least one encryption key pair includes the step of producing the at least one additional signature key pair, and

the user marks a public part of the at least one additional signature key pair using the secret part of the previously generated signature key pair.

6. (New) The method according to claim 5, further comprising the steps of:

in each bilateral communication occurring between a user desiring no communication with the trust center and another user, marking and making available to the other user one of the public part of the at least one encryption key pair and the public part of the at least one additional signature key pair by using the secret part of the previously generated signature key pair; and

checking a correctness of an assignment regarding one of the public part of the at least one encryption key pair and the public part of the at least one additional signature key pair by performing the steps of:

verifying a signature, and

checking a genuineness and a validity of the new certificate in the trust center.--.

In The Abstract:

Delete the present Abstract and in its place insert the following:

--Abstract Of The Disclosure

A method in which a user first receives from a Trust Center a generated, personalized, and certified key pair as well as components for producing encryption pairs. The user at any time himself produces an encryption key pair, marks the public part of this pair using the secret signature key relinquished to him, and transmits the result to the Trust Center, where the result is assigned to the user using the certified public part of the signature key pair.--.

Remarks

This Preliminary Amendment cancels claims 1-3 in the underlying PCT Application No. PCT/EP98/07984, and adds new claims 4-6. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification and abstract are to conform the specification and abstract to U.S. Patent and Trademark Office rules. The amendments to the specification and abstract do not introduce new matter into the application.

The underlying PCT application includes a Search Report dated May 6, 1999, a copy of which is submitted herewith.

Applicants assert that the present invention is new, non-obvious, and useful. Consideration and allowance of the claims are requested.

Respectfully submitted,

KENYON & KENYON

By: Dena Magnuk
(Reg. No. 47,172)

Dated: 9/13/99

By: Richard L. Mayer
Richard L. Mayer
Reg. No. 22,490

One Broadway
New York, NY 10004
(212) 425-7200

214530

A METHOD FOR GENERATING ASYMMETRICAL CRYPTOKEYS AT THE USER'S LOCATION

Background Information

The invention relates to an asymmetrical cryptological method of the type described in more detail in the preamble of patent Claim 1. Methods of this type are widely known and are described, e.g., in Menezes: Handbook of Applied Cryptography, 1997.

A crucial problem of all known open cryptological methods is the reliable assignment to the authorized user of the utilized signature and encryption keys and the confirmation of the assignment by an independent third entity. In technical terms, this is a question of the reliable personalization of the keys along with subsequent certification.

Trustworthy methods, such as are described by Kowalski, in The Telecommunications Engineer 4/5 1995: "Security Management System," solve this problem currently by generating, personalizing, and certifying keys of this type at a central, particularly secure location (usually so-called Trust Centers).

However, it cannot be excluded that in the future the users themselves will increasingly wish to generate their cryptokeys, in particular those for encryption. This desire should not be realized at the expense of the security and reliability of the method in question, as is the case today in the only loosely organized asymmetrical cryptological methods of the Internet.

Thus as the objective of the invention, a method is required which shifts the generation of keys into the area of responsibility of the user without forfeiting the organizational security of an independent entity.

This objective is achieved in the method indicated in the characterizing part of Patent Claim 1.

Advantageous possibilities for refinements are apparent in the characterizing part of Subclaim 2.

The invention is explained on the basis of the following exemplary embodiment:

The user receives from the central location, hereinafter termed Trust Center, a signature key pair that is already generated, personalized, and certified, e.g., a private signature key PS and a public signature key ÖS as well as the components for producing one or more encryption key pairs, Generate Encryption Keys, GEK.

The user then himself produces at any time an encryption key pair, e.g., a private encryption key PVS, marks the public part of this pair, public encryption key OVS, using the previously relinquished secret signature key PS, and transmits the result to the Trust Center. There, using a check with the aid of the certified public part of the signature key pair ÖS of the user, the result is to be assigned as belonging, unequivocally and reliably, to the user.

The Trust Center thereupon generates a new certificate, in which are contained either both the public part of signature key pair ÖS as well as that of encryption key pair ÖVS, or only that of the encryption key pair ÖVS of the user.

This certificate, in the next step, is then encrypted using the public part of the encryption key pair ÖVS of the user and is then transmitted.

Thus it is assured that only the authorized user is able to decode the certificate and, in hardware-based systems, can download it into his corresponding hardware. At no time does the user have to reveal his secret, namely the secret part of encryption key pair PVS.

If the user also wishes to generate the signature key pair in his area of responsibility, in other words if he also wants to protect the secret part of a signature key pair, a second private signature key PS2, from being accessed by the Trust Center, then this method is also used analogously for this purpose. Only the components Generate Digital Signature Keys, GDSK, for producing one or

more signature key pairs, are also relinquished to the user.

Once generated, with the aid of the secret signature key PS relinquished by the Trust Center, the user also marks the public part of self-generated signature key pair ÖS2, in addition to or simultaneous with the public part of self-generated encryption pair ÖVS, and the result is transmitted to the Trust Center, where subsequently the process is continued just as described above.

If user AW1 does not wish to have any further communication with a Trust Center, he can do this as well using the described method without any loss of reliability, by first marking and making available to the communication partner the public part of his self-generated key pair ÖVS using the secret part of the previously relinquished, personalized, and certified key pair PS in every bilateral communication with another user AW2.

Receiving communication partner AW2 can reliably check the correct assignment of this information with regard to public part ÖVS of the key pair self-generated by sending user AW1 by verifying the signature and, if necessary, checking the genuineness and validity of the certificate in the Trust Center underlying this signature.

Patent Claims

1. A method for generating asymmetrical cryptokeys at the user's location, in which keys are generated, personalized, and certified at a central, particularly secure location, (Trust Center), or, in cooperation using secure transmission between the user and this Trust Center, at the location of the user,

characterized in that

a. first, the user is provided by the Trust Center with a previously generated, personalized, and certified signature key pair (PS, ÖS), and also components for producing one or more encryption key pairs (GEK),

b. thereupon, a further user's-own encryption key pair having a public (ÖVS) and a secret part (PVS) is produced by the user, and the public part (ÖVS) is marked using the assigned secret part (PS) of the signature key and the result is transmitted to the Trust Center,

c. thereupon, the unequivocal assignment to the user is checked by the Trust Center using the certified public part (ÖS) of the signature key pair,

d. after a successful check of the assignment, a new certificate is produced by the Trust Center using at least a public part of the signature key pair (ÖS) or of the encryption key pair (ÖVS) of the user, and finally

e. this certificate, encrypted using the public part of the encryption key pair (ÖVS) of the user, is transmitted by the Trust Center to the user.

2. The method for generating asymmetrical cryptokeys at the user's location as recited in Claim 1, characterized in that the user, in method step a., is additionally provided with components (GDSK) for producing one or more signature key pairs, which, in method step b., are also produced by the user, and that the public part (ÖS2) of this self-generated signature key pair is marked by the user, in addition or simultaneously, using the secret part of the signature key pair (PS) received from the Trust Center.

3. The method for generating asymmetrical cryptokeys at the user's location as recited in Claim 1 and 2,

characterized in that a user (AW1) desiring no communication whatsoever with a Trust Center, in every bilateral communication with another user (AW2), first marks and makes available to the latter the public part of his self-generated key pair (ÖVS or ÖS2) using the secret part of the key pair (PS) previously relinquished, personalized, and certified by the Trust Center, whereupon the correct assignment of this information regarding the public part (ÖVS or ÖS2) of the key pair self-generated by the sending user (AW1) is checked by the receiving user (AW2) by verifying the signature, and the genuineness and validity of the certificate in the Trust Center underlying this signature can be checked.

Abstract of the Disclosure

2.1 In generating asymmetrical cryptokeys in the handwriting of the user, signature and encryption keys are necessary, and in personalizing and certifying, reliable connections to a Trust Center are necessary. If users wish to generate their own keys, particularly cryptokeys, security problems arise.

2.2 Problems of this type are reduced by a method in which the user first receives from the Trust Center a generated, personalized, and certified key pair as well as components for producing encryption pairs. The user at any time himself produces an encryption key pair, marks the public part of this pair using the secret signature key relinquished to him, and transmits the result to the Trust Center, where the result is assigned to the user using the certified public part of the signature key pair.

2.3 The area of application of the invention includes all forms of asymmetrical cryptological methods: essentially, ATM cards/bank transactions, access controls to networks/databases, entry controls to buildings/rooms, digital signatures, digital IDs/patient cards.

2345/86

COMBINED DECLARATION AND
POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below adjacent to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **A METHOD FOR GENERATING ASYMMETRICAL CRYPTOKEYS AT THE USER'S LOCATION;**, and the specification of which:

[ ] is attached hereto;

[ ] was filed as United States Application Serial No. _____ on _____, 19__ and was amended by the Preliminary Amendment filed on _____, 19__.

[X] was filed as PCT International Application Number PCT/EP98/07984, on the 9th day of December, 1998.

[X] an English translation of which is filed herewith.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a). I hereby claim foreign priority benefits under Title 35, United States Code § 119 of any foreign application(s) for patent or inventor's certificate or of any PCT international applications(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a

filing date before that of the application(s) of which priority is claimed:

PRIOR FOREIGN/PCT APPLICATION(S)
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. § 119

Country : Germany

Application No. : 198 01 241.1

Date of Filing: January 12, 1998

Priority Claimed
Under 35 U.S.C. § 119 : [X] Yes [ ] No

I hereby claim the benefit under Title 35, United States Code § 120 of any United States Application or PCT International Application designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations § 1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application:

PRIOR U.S. APPLICATIONS OR
PCT INTERNATIONAL APPLICATIONS
DESIGNATING THE U.S. FOR BENEFIT UNDER 35 U.S.C. § 120

U.S. APPLICATIONS

Number :

Filing Date :

PCT APPLICATIONS
DESIGNATING THE U.S.

PCT Number :

PCT Filing Date :

I hereby appoint the following attorney(s) and/or agents to prosecute the above-identified application and transact all business in the Patent and Trademark Office connected therewith.

(List name(s) and registration number(s)):

Richard L. Mayer,	Reg. No. 22,490
Gerard A. Messina,	Reg. No. 35,952
_____,	Reg. No. _____
_____,	Reg. No. _____

All correspondence should be sent to:

Richard L. Mayer, Esq.
Kenyon & Kenyon
One Broadway
New York, New York 10004

Telephone No.: (212) 425-7200
Facsimile No.: (212) 425-5288

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

1-00

Full name of inventor Paul MERTES

Inventor's signature _____ Date 9/16/99

Citizenship Federal Republic of Germany

Residence Mertenseifer Grund 9
D-57258 Freudenberg
Federal Republic of Germany DEX

Post Office Address Same as above

2-00

Full name of inventor Werner METTKEN

Inventor's signature _____ Date 04.12.99

Citizenship Federal Republic of Germany

Residence Eichenweg 9
D-59969 Hallenberg
Federal Republic of Germany DEX

Post Office Address Same as above

214508